High Fairness Reader Anti-Collision Protocol in Passive RFID Systems

Carlo Galiotto, Kamil Cetin, Simone Frattasi, Nicola Marchetti, Neeli Rashmi Prasad, Ramjee Prasad
Center for TeleInFrastruktur (CTIF), Aalborg University, Denmark
{cg,kc,sf,nm,np,prasad}@es.aau.dk

***Abstract*—With the spread of passive Radio Frequency Identification (RFID) systems, new applications will see the coexistence of more and more RFID readers in the same area. As for wireless devices, also RFID readers experience collisions whenever sharing the same communication channel. In this paper, an anti-collision protocol has been proposed in order to solve the reader collision problem. The aims of the proposed solution are: (1) to prevent and avoid collisions among readers; and (2) to limit the access delay of the readers on the channel, while guaranteeing them fairness with respect to the channel contention. The reader anti-collision here proposed, referred as to High Fairness Reader Anti-Collision Protocol (HF-RACP), has been designed taking into account passive tags and their limitations in terms of computational and frequency selectivity capabilities. In this paper, after presenting the reader collision problem and discussing the simulation models and the evaluation methodology used herein, the simulation results for several anti-collision algorithms are shown in terms of collision avoidance and access delay. The comparison with contention-based schemes, like Listen Before Talk (LBT), demonstrates that HF-RACP is more effective against collisions, improves the fairness among readers and considerably reduces the maximum access delay.**

***Index Terms*—Access delay, anti-collision protocol, fairness, RFID, reader.**

I. Introduction

Even though RFID systems are increasingly spreading, some issues related to their reliability still need to be solved. Indeed, RFID readers can experience misreads during the tag identification process. One of the causes of such a problem is the occurance of collisions, which may happen both at readers and tags. In general, collisions occur when multiple devices try to access the same channel at the same time [1].

The collisions experienced within RFID systems are classified in two categories. The first type of collision occurs when a reader simultaneously communicates with two or more tags [1]; this is referred to as tag-to-tag collision or *tag collision problem*. For the tag collision problem some solutions have already been proposed in the standard EPC C1G2 [2]. The second type of collision occurs when two or more readers simultaneously communicate with one or more tags [3], [4]; this is referred to as *reader collision problem* (see Fig. 1). In fact, in the reader collision problem the interferer is represented by a reader, while the interfered victim can be either a reader (i.e., reader-to-reader collision, Fig. 1, center) or a tag (i.e., reader-to-tag collision, Fig. 1, right-hand side). In case of passive RFID systems, the design of an anti-collision scheme must consider the limitation imposed by passive tags,

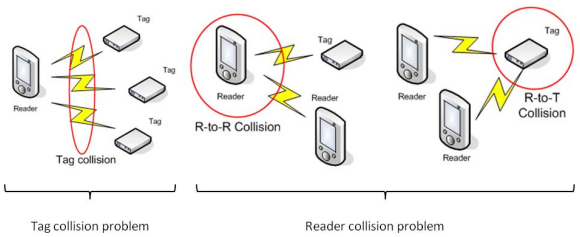

Fig. 1: Tag collision (left-hand side); reader-to-reader collision (center); and reader-to-tag collision (right-hand side).

i.e., that of not including a battery. For this reason and also in order to guarantee a low production cost, passive tags have simple electronics [5]. As a consequence, [3]: (a) they do not have filtering capabilities; (b) they cannot solve heavy computational tasks; and (c) they are not autonomous devices, which can operate without the control of the readers.

In this paper, only the *reader collision problem* will be considered. After explaining the reader collision problem and presenting the models used for our simulative analysis, we propose a reader anti-collision protocol that may represent an effective solution to the reader collision problem in passive RFID systems. Differently from previous solutions (i.e., [3]-[6]) our protocol tries to lower the access delay of the readers while guaranteeing them fairness during the channel contention phase. The access delay has in fact not been targeted as a goal for the anti-collision algorithms available in the literature. However, reducing the waiting time of the readers turns out to be a crucial parameter in those applications that require a high reactivity of the readers, such as check points in warehouses and convey lines, or tracking of mobile tags.

The paper is organized as follows. The state-of-the-art of anti-collision protocols is presented in Section II. In Section III, we introduce our solution. Section V illustrates the simulation models and the simulation results. Finally, our concluding remarks are drawn in Section VI.

II. Related works

Due to the above limitations imposed by passive tags, some existing Medium Access Control (MAC) techniques cannot be employed as a basis for designing anti-collision protocols in passive RFID systems. For example, Frequency Division

Multiple Access (FDMA) requires filtering capabilities [3]; Code Division Multiple Access (CDMA) is computationally heavy from an implementation point of view [3] and Space Division Multiple Access (SDMA) [7] is an expensive solution as it requires complex antenna design. Time Division Multiple Access (TDMA) seems to be the only MAC technique applicable to passive RFID systems, even though the issue of synchronization among readers shall be taken into account. In fact, in order to make TDMA effective, the readers should be synchronized by means of a communication protocol employed, for example, between the readers and a control unit (e.g., a central server). Hereafter, we present a review of the state-of-the-art of the reader anti-collision protocols.

1) Listen Before Talk (LBT): The European Telecommunications Standard Institute (ETSI) with the standard "ETSI EN 302 208-1 0" [8] requires RFID readers operating in the band between 865 MHz and 868 MHz to listen to the channel before transmitting, so as to prevent mutual interferences and thus collisions. This basic form of anti-collision protocol is referred to as LBT and is carrier-sense-based, like the Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA) implemented in IEEE 802.11. However, the carrier-sense-based anti-collision algorithms are regarded as non-effective against the hidden terminal problem affecting the passive RFID systems [3].

2) Colorwave: Colorwave [9] is a TDMA-based method where the time is divided in frames and each frame has a given number of slots (also referred to as "colors"). Each reader picks up one of these colors within the frame and transmits only during that slot. Whenever a collision is detected, a reader chooses a different time slot within the frame and communicates such a change to its neighbor readers, so that the latter can be aware of the update and change their own colors inside the frame. The method for synchronizing the readers is not specified but it can be achieved, for instace, by using a clock onboard the readers [9]. However, Colorwave relies on the collision detection, which cannot be performed unless the tags are involved in this process.

3) Pulse: Pulse [3], proposed for mobile RFID reader scenarios, is a distributed algorithm that aims at resolving the hidden terminal problem typical of CSMA-based algorithms. Two non-interfering channels are used by the readers. The first one (control channel) is reserved for reader-to-reader communications, while the second one (data channel) is employed for reader-to-tag communications. When transmitting on the data-channel, the reader broadcasts beacon messages over the control channel in order to inform the potentially colliding readers that the data channel is busy. However, being a contention-based method, the performance of Pulse in terms of access delay is supposed to decrease when the density of the readers contending the channel increases.

Some other anti-collision algorithms have been derived from Pulse [3]. In [10], a modification of Pulse is proposed in order to decrease the access delay of the algorithm by adaptively changing the beacon range according to the readers' density. In [11], the readers are signaling their own transmissions to the other readers over a control channel (like in Pulse). However, a central server is in charge of organizing a semi-distributed resource allocation algorithm. Each reader thus follows the commands transmitted by the server and also transmits a beacon in order to identify collisions with neighbor readers.

4) Slotted LBT: This algorithm [12] applies the LBT algorithm (see Section II-1) for accessing multiple channels. In case a channel is sensed to be busy, a new channel is considered for transmissions. Slotted-LBT requires the readers to be synchronized. Synchronization is carried out by one of the readers which acts as a master within the cluster, while the other readers act as slaves. However, the usage of different channels is not useful to reduce the interference from the readers to the tags, since the latter do not have filtering capabilities.

III. High Fairness Reader Anti-Collision Protocol

HF-RACP is a TDMA-based centralized reader anti-collision protocol, which schedules the readers with the aim of providing them a good fairness during the channel contention phase, i.e., all the readers will have a fair opportunity to access the channel.

The usage of a centralized scheduling for reader anti-collision purposes has also been object of our previous work [13], where we proposed a centralized scheduling carried out by a Central Unit (CU) and based on the outcome of a collision discovery algorithm (see Section III-A). However, as the goal of HF-RACP is to increase the fairness among readers rather than only limiting their average access delay (as it was done in [13]), the scheduling is performed in a diffent way with respect to [13].

The idea behind the usage of a centralized system arises from the usual networking infrastructure of RFID systems, which can be in fact considered centralized. Indeed, readers are usually connected to a CU, where the data they have received from the tags is uploaded. It is thus assumed that there exists a link between the CU and each reader, which can be used to control the reader itself. Furthermore, in [13], it has been pointed out that the use of a centralized anti-collision algorithm reduces the access delay of the readers to the channel.

HF-RACP has been designed considering the constraints imposed by passive tags in terms of computational and frequency filtering capabilities (see Section II), which do not allow using Frequency Division Multiple Access (FDMA), CDMA and SDMA techniques as a basis for designing anti-collision protocols in passive RFID systems.

HF-RACP schedules the readers based on the channel availability (i.e., the channel is busy if at least one reader is currently transmitting) and the demand of the readers for accessing it. In order to perform this action though, it needs to know which readers are potentially colliding. Hence, it needs to accomplish two different tasks. First, it has to discover the potential collision occurrences among readers. Second, it shall perform the scheduling of the readers. Hence, HF-RACP consists of a *collision discovery algorithm* and a *scheduling*

algorithm, which are described in details in the following subsections.

A. Collision Discovery Algorithm

This protocol requires that the readers to broadcast a control beacon. Basically, all the readers receiving the beacon from one of their neighbors are considered potentially colliding with that reader.

By tuning the sensitivity of the receivers, $P_{S,beacon}$, only the readers that are within a certain distance will detect the beacon. Hence, they will be considered as potentially colliding. $P_{S,beacon}$ should be set in such a way that, if the received power of the beacon is greater than the threshold $P_{S,beacon}$, the interference experienced from the sending reader could cause a collision at the receiver. The value of $P_{S,beacon}$ has been set to -96 dBm, which is the sensitivity threshold used in LBT (see Section IV-B2).

Note that the idea of using this broadcasting phase for collision discovery purposes was already introduced in [3]. As Birari proposes [3], the beacon should be sent over a channel which is spectrally separated from the channel used for reader-to-tag communications. These two channels are referred to as "control channel" (i.e., the one for beacon broadcasting) and "data channel" (i.e., the one used for reader-to-tag communications). Furthermore, the beacon should contain a given number or code representing the sender (e.g., sender ID), so that the receiving reader can identify the sender, that is, the potentially colliding reader.

The outcome of the collision discovery algorithm is a collision graph (see Fig. 2), i.e, a graph where the readers (the vertices of the graph) are connected by an edge in case they are considered potentially colliding (in Fig. 2, R_1 and R_3 represent potentially colliding readers), while readers which are not potentially colliding are represented as unconnected vertices (in Fig. 2, R_2 and R_{10} represent non-colliding readers).

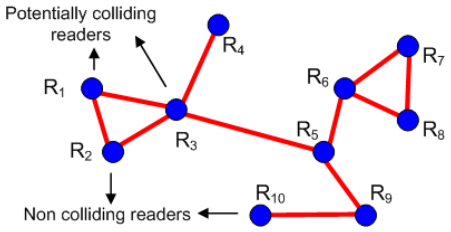

Fig. 2: Collision graph.

Since the protocol is centralized, the collision discovery algorithm must run both at the readers and at the CU. As for the reader side of the algorithm, each reader has to transmit a beacon whenever the CU sends a request. The readers receiving this beacon (i.e., whose received power is higher than the threshold $P_{S,beacon}$) forward to the CU the ID of the reader that has transmitted the beacon. The pseudo-code of the collision discovery algorithm implemented in the readers is reported in Fig. 3.

As for the CU side of the algorithm, the CU has to issue the "send beacon request" to the readers for sending in turn a beacon. At each interval T_{beacon} only one reader will send the beacon. Thus, if N is the total number of readers in the system, each reader will send a beacon periodically every $N \cdot T_{beacon}$ seconds.

CASE: "CU issues *send beacon request*"

1. Each reader broadcasts a beacon packet over the control channel.

CASE: "Signal detected over the control channel"

1. If the power of the received signal $P_{RX,beacon}$ is higher than $P_{S,beacon}$, decode the beacon message and report the ID of the sender to the CU.
2. If $P_{RX,beacon} \leq P_{S,beacon}$, discard the message.

Fig. 3: Collision discovery algorithm - reader side.

INITIALIZATION: $N_r = 0$, where N_r is the index of the last reader transmitting the beacon.

CASE: "Beacon timeout expired"

1. Request the reader with index $N_{ind} = N_r + 1$ to transmit the beacon.
2. $N_r = REM(N_r + 1, N)$.
3. Wait for time $T_{readerReply}$.
4. For any reader R_c reporting the ID of the sender, insert an edge between R_c and the sender in the collision graph.
5. For any reader R_{nc} not reporting the ID of the sender, remove the edge between R_{nc} and the sender in the collision graph (if there is such an edge).

Fig. 4: Collision discovery algorithm - CU side.

REM in Fig. 4, step 2, denotes the Remainder After Division operation. After waiting an interval $T_{readerReply}$, necessary for the readers to receive the beacon, process the message and reply to the CU, the latter updates the collision graph based on the readers' feedback. The pseudo-code of the collision discovery algorithm implemented in the CU is reported in Fig. 4.

B. Scheduling Algorithm

The scheduling algorithm makes use of the collision graph built and constantly updated by the collision discovery algorithm in order to dynamically schedule the readers in the data channel. As mentioned previously, the readers are scheduled based on the availability of the channel and the demand of the readers for accessing it.

The aim of the scheduling algorithm is twofold. The first objective is to avoid collisions among readers. The second one is to reduce the access delay of the readers to the channel, while at the same time guaranteeing fairness among the readers

when accessing it. In order to ensure that no collision occurs, the algorithm is allowed to schedule simultaneously multiple readers only if they are regarded as not potentially colliding. Each time there is an opportunity to allocate a new reader, the CU chooses the reader which is experiencing the highest access delay. In this way, each time a reader is not allocated, its delay rises and thus its probability of being allocated in the next turn increases. Hence, by allocating the readers with the highest delays, we aim at providing a certain degree of fairness among the readers. Furthermore, since the reader with the highest delay metric has priority over the other readers, this algorithm also reduces the maximum access delay of the system.

The algorithm uses two metrics for delay comparison among readers. The first one, referred to as Mean Waiting Time (MWT), is computed for all the readers and is updated each time the reader is allocated. The MWT is updated as follows:

$$MWT_{new} = (1 - \alpha)MWT_{old} + \alpha LWT, \quad (1)$$

where the Latest Waiting Time (LWT) is the waiting time experienced by the reader before its latest allocation and α is a factor that weights the past waiting time MWT_{old} with the LWT. The second metric, referred to as access delay metric (ADM), is computed only for the readers that are in a "waiting state" (i.e., the readers that asked for accessing the channel and are waiting for the channel to become idle). The ADM is defined as follows:

$$ADM = (1 - \beta)MWT + \beta CWT, \quad (2)$$

where the current waiting time (CWT) is the time currently spent by the reader in its "waiting state" and β is factor that weights the MWT and the CWT. The pseudo-code of the scheduling algorithm is reported in Fig. 5.

VARIABLES:

- T: is the set of readers in "transmitting state".
- W: is the set of readers in "waiting state".

INITIALIZATION

1. The two sets T and W are empty.

CASE: "A reader R requires to access the channel"

1. Check if reader R is potentially colliding with any of the readers in T.
2. If so, set R in "waiting state".
3. Otherwise:
   - 3a. Find the neighbors of R in waiting state.
   - 3b. Check if reader R has MWT higher than the MWT of its neighbors in waiting state.
   - 3c. If so, set R in "transmitting state".
   - 3d. Otherwise, set R in "waiting state".

CASE: "A reader R_q leaves the channel"

I. Among the readers in waiting state, find the ones which do not collide with any of the readers in T.
II. Among the readers found in Step I., find the reader $R_{candidate}$ with maximum ADM.
III. Among the readers found in Step I., find the largest set $S_{candidate}$ of readers not colliding with $R_{candidate}$.
IV. Set readers in $S_{candidate}$ and the reader $R_{candidate}$ in "transmitting state" and update their MWTs.

Fig. 5: Scheduling algorithm.

IV. Simulation Methodology

In this section, we present the simulation models and parameters used to obtain the simulation results (see Section V), and the anti-collision algorithms taken as a reference against our solution.

A. Simulation Models and Parameters

1) Scenarios: Three different scenarios are considered for our simulative analysis. In *Scenario 1*, 20 readers and 400 tags are randomly and uniformly deployed in an indoor environment represented by a square room (30 m x 30 m). With this scenario we aim at testing how the anti-collision algorithms work in a general case of random deployment of readers and tags in an indoor environment.

In *Scenario 2*, 9 readers are randomly and uniformly deployed within a square room (30 m x 30 m), while 10 tags are randomly placed within a circle of maximum radius 1 m and minimum radius 40 cm, centered on each reader. With this scenario we aim at simulating how the anti-collision algorithms work when the readers are in proximity of the tags. In such a situation, it is expected that the readers are less sensitive to the interference, since the tags are closer to the interrogator and thus the received signal strength is higher.

Scenario 3 consists of an indoor environment including 9 square rooms (10 m x 10 m), each divided by a wall. In each room we consider one reader and for each reader 10 tags. The position of the readers is randomly defined within each room, while the tags are randomly placed within a circle of maximum radius 1 m and minimum radius 40 cm, centered on each reader. With this scenario we aim at simulating the effect introduced by the walls on the mutual interference of the readers with respect to *Scenario 2*.

2) Channel Models: Since the passive RFID systems that we are considering work in the ultra-high frequency (UHF) band and can be used in the band ranging from 840 MHz to 960 MHz [14], we set the carrier frequency, f_c , at 900 MHz. In our simulations, we use an indoor channel model valid for a carrier frequency set at 900 MHz. Both far-field and near-field channel models are taken into account.

a) Near-Field: No multipath fading and shadowing are taken into account for the near-field channel model. The reasons for this assumption are the following: (i) Multipath fading and shadowing describe attenuation phenomena related to the far-field model [15]; (ii) In [16], it is shown that the multi-ray channel model does not have relevant differences with respect to the free-space path-loss formula for a distance lower than 1 - 1.5 m; (iii) in [17], it is shown that the path-loss model in the near-field matches with the experimental measures as long as the distance d from Tx to Rx is not lower than $\lambda \div 1.5\lambda$ [17], where λ is the wavelength.

Therefore, we use as channel model for the near-field only the path-loss, which is defined by [18]:

$$PL(d) = 32 + 25\log_{10}(d), \quad \lambda \leq d \leq d_m, \tag{3}$$

where d_m is the break-point distance between the near-field and the far-field channel models, whose value will be discuused later in Section IV-A2b.

Note that, since this model is not valid for distances shorter than $\sim \lambda \div 1.5\lambda$ (i.e., 33-50 cm for f_c = 900 MHz), the tags are placed at a minimum distance of 40 cm from the reader.

b) Far-Field: For the far-field, the channel model includes path-loss and Rayleigh distributed multipath fading. A similar approach for modelling the far-field channel model has been considered in [19], where only path-loss and multipath fading have been taken into account. The model used for path loss $PL(d)$ is given by [18]:

$$PL(d)_{dB} = \begin{cases} 32 + 25\log_{10}(d), & \lambda \leq d \leq d_m, \\ 23 + 25\log_{10}(d), & d \leq d_m, \end{cases} \tag{4}$$

In the literature, no explicit value of d_m is given. However, it could be inferred from [[16], pg. 7, Fig. 8a] that possible values for d_m range from 1 m to 2 m.

c) Wall Attenuation: The wall attenuation is considered to be additive to the path-loss. The attenuation provided by one wall depends on its thickness. [20] gives 8-15 dB.

d) Transmitted and received power: When the reader transmits to a tag with a given power $P_{tx,R}$, the tags receives a certain power $P_{rx,T}$ depending on the channel path-loss and on the reader and tag's antenna gain. In UHF passive systems, only a part η_{eff} of the recieved power $P_{rx,T}$ is backscattered from the tag to the reader. Hence, the power transmitted by the tag is $P_{tx,T} = \eta_{eff} P_{rx,T}$, where η_{eff} is referred to as *modulation efficiency* [21]. In order to power up the chip in a tag, $P_{rx,T}$ must not be lower than the "power sensitivity of the tag", $P_{sens,T}$, which is the minimum power required by a tag to work.

3) Determining Collsion Occurances at the Physical Layer: In the simulator, in order to evaluate if a collision occurs, we consider the probability that the packets exchanged between readers and tags are error-free. If we transmit a packet of L_{packet} bits from the Tx to the Rx, under the assumption of independent and identically distributed (i.i.d.) bits, the probability that all the bits are correct is $P_{pck} = (1 - P_{bit})^{L_{packet}}$, where P_{bit} is the bit error probability. It is assumed that the reader to tag link (*forward link*) uses binary Amplitude Shift Keying (ASK) modulation and the tag to reader link (*reverse link*) uses Binary Phase Shift Keying (BPSK) [2]. For such modulations, assuming an Additive White Gaussian Noise (AWGN) channel, P_{bit} is a function of the Signal to Noise Ratio (SNR) (i.e., $P_{bit} = f(\text{SNR})$), whose formulation can be found in [15]. In order to take into account the effect of the reader interference on P_{bit}, we sum the power of the interference and the noise power, i.e., we compute the Signal to Interference plus Noise Ratio (SINR) [22] and then we obtain the bit error probability as $P_{bit} = f(\text{SINR})$.

Concerning the length L_{packet} of the packets exchanged between readers and tags, we consider for the forward link the sum of the lengths of each packet transmitted from the reader to the tag and then, since no retransmission scheme is currently implemented in the simulator, we assume that this communication is successful if each packet is received correctly by the tag. The sum of the packet lengths transmitted from the reader to the tags is 94 bits [2]. The same considerations are valid for the reverse link, for which the sum of the packets lengths ranges from 41 up to 548 bits [2]. In our simulations we have set this value to 200 bits.

In order to make the communication link between tags and reader more robust against noise or interference, we used channel coding (e.g. Hamming (7,4) [23]). By transmitting at the same power (at the tag) and at the same data rate, we aim at reducing the bit error probability of the transmission for the same SNR value measured at the receiver. This is paid by increasing the time needed to transmit the information packet of a given length. Let us note that, due to computational capabilities and power constraints of passive tags, the channel coding is applied only to the reverse link. In fact, the Hamming (7,4) encoding process is computationally simple and is not energy expensive and thus can be implemented in the tags [24]. On the other hand, the decoding process, which is more computational expensive and power consuming, is implemeneted in the readers, where an active power source is available [24].

B. Anti-Collision Algorithms for Performance Comparison

In this subsection, the parameters of the anti-collision algorithms used for performance comparison are reported. These algorithms are Aloha, LBT [8] and an adaptation to RFID systems of CSMA/CA.

1) ALOHA: it is based on the free access to the transmission channel, without caring if the transmission channel is busy or not. The access to the channel is done each time the application requires the reader to interrogate the tags. This request is generated with an exponential arrival time τ_{arr} (Poisson arrival model) [3]; this parameter should be chosen in accordance with the average time required by the readers to interrogate the tags (the reading time t_r per tag is 3 ms [19]). In fact, τ_{arr} would need to be at least greater than the time required by the reader to interrogate the tags, i.e. $\tau_{arr} > n_{tag} \cdot t_r$, where n_{tag} represents the number of tags to be read by the reader. By comparing HF-RACP with Aloha we want to evaluate the improvement in terms of collision avoidace of our proposal with respect to the case where no channel access control is used.

2) LBT: Since we want to evaluate the improvement of HF-RACP in terms of collision avoidace and in terms of access delay with respect to a protocol which is already used in the RFID systems, we compared our proposal with LBT, which is defined by the standard "ETSI EN 302 208-1 0" (see Section II-1). LBT defines both the listening time and the power threshold for carrier sensing. The listening time τ_{lis} is defined as $\tau_{lis} = 5ms + \tau_{rand}$, where τ_{rand} is a random

TABLE I: Sensed Power Thresholds for LBT [8].

Transmit Power	Threshold (e.r.p.)
Up to 100 mW	≤ -83 dBm
101 mW to 500 mW	≤ -90 dBm
501 mW to 2 W	≤ -96 dBm

time chosen in the range [0, 5] ms, with steps of 0.5 ms. This counter can be decreased only when the channel is sensed to be idle. The thresholds for the carrier sensing are shown in Table I.

3) CSMA/CA: Several anti-collision solutions proposed in the literature (see Section II) protocols are CSMA-based protocols. Hence, in order to evaluate the improvement in terms of collision avoidace and in terms of access delay of HF-RACP with respect to CSMA based anti-collision protocols, we compare HF-RACP with CSMA/CA. The CSMA/CA implemented in the simulator has been derived from the same MAC scheme used in the standard IEEE 802.11 (basic access) [25], but with different parameters. The parameters which need to be re-set in order to adapt CSMA/CA to the standard are the Distributed Inter-Frame Space (DIFS) length (i.e., time interval during which the channel has to be sensed as idle by the reader before accessing the channel), the minimum (CW_{min}) and maximum (CW_{max}) lengths of the congestion window for the back-off algorithm. The values of DIFS, CW_{min} and CW_{max} depend on some physical layer parameters of IEEE 802.11 [25]. Since the physical layer of the RFID readers is different from the physical layer defined for the standard IEEE 802.11, in our simulation we chose to use the values of DIFS, CW_{min} and CW_{max} from [3], where the authors have adapted the CSMA/CA back-off algorithm of IEEE 802.11 to an anti-collision algorithm for readers (Pulse, see Section II-3). These parameters are reported in Table II.

As far as it concerns the thresholds for the carrier sensing, since LBT is a carrier-sense-based algorithm, the values reported for LBT (see Table I) can also be used for the CSMA/CA.

C. Implementation Parameters for HF-RACP

As far as it concerns the collision discovery algorithm, two parameters must be set. The first one is the beacon time interval T_{beacon}, the second one is the beacon sensitivity $P_{S,beacon}$ in the reader.

The beacon time interval (which is inversely proportional to the update rate of the collision graph) is given by a trade-off. The higher is the rate, the faster is the update of the collision graph and the higher is the overhead introduced by the algorithm. The value of T_{beacon} becomes especially important if the mobility of the readers is taken into account, as with the mobility the readers change their position and thus also the collision graph must be updated accordingly.

Since in our simulations the readers are considered to be static, basically the collision graph never changes. Thus, T_{beacon} only needs to be much shorter than the simulation time, so that the collision graph is built sufficiently before the simulation finishes (i.e., as long as the collision graph is not built, the anti-collision protocol is still in its transient time). In our case, we set T_{beacon} to be 0.5 s.

The beacon sensitivity has been set to -96 dBm, which is the same sensitivity threshold set for LBT and CSMA. As far as it concerns the scheduling algorithm, the parameters α and β have been set empirically in our simulations to 0.5 and 0.3.

V. Simulation Results

In this section, we present the simulation results of the proposed anti-collision protocol compared to Aloha, LBT and CSMA.

Four different metrics have been taken into account. The first one, the *collision avoidance efficiency*, is defined as the percentage of tags correctly read by all the readers in the considered scenario. The remaining metrics are three types of access delay metrics, which determine the delay of the readers in accessing the channel. These three metrics are: (1) the *average access delay*; (2) the *standard deviation* of the average access delay; and (3) the *maximum access delay*. The average access delay gives a measure of the average time the readers shall wait before transmitting because of the occupancy of the channel. The standard deviation of the average access delay gives a measure of the fairness of the algorithm with respect to the scheduling of the readers. The higher this parameter, the bigger is the difference among the mean access delays of the different readers and thus the lower is the fairness of the system.

At each simulation snapshot new positions for readers and tags are drawn. The simulation comparison has been carried out for the three different scenarios illustrated in Section IV-A1. The summary of the values of the parameters used in the simulations is shown in Table II. The bar plot in Fig. 6 shows the simulation results concerning the collision avoidance efficiency of the compared algorithms. As it can be seen from the plot, we can derive that: (1) Aloha has a really low anti-collision efficiency. From these results it could be inferred that Aloha is practically useless against collisions, unless the readers are separated by walls, as in this case the interference from other readers is reduced; (2) LBT has an anti-collision efficiency that strongly varies based on the scenario; it reaches a maximum of 86%; (3) CSMA has also a good collision avoidance efficiency, which ranges between 93% and 99%; and (4) the anti-collision method performing better is HF-RACP. As it can be noticed, the anti-collision performance of the algorithms varies based on the considered scenario. In fact, in Scenario 1, where readers and tags are deployed randomly in the indoor environment, Aloha, LBT and CSMA show the worst performance. In Scenario 2, since the tags are placed around the readers, the strength of the signal received both by the tags and the readers is higher and thus the receiver is more immune to interference. In Scenario 3, the effect of the walls on the interference attenuation is evident. In fact, since each reader is placed in a different room, the wall separating the different rooms attenuates the interference coming from the neighboring rooms. Due to this limited jamming, readers experience fewer collisions.

TABLE II: Summary of the parameters used in the simulations.

General Parameters	
Simulation time	300 sec.
Number of simulations	100
Channel and Physical Layer Parameters	
Carrier Frequency	900 MHz
$P_{tx,R}$	1 W [16],[14]
η_{eff}	0.25 [21]
Reader antenna gain, G_R	0 dBi (omni-directional)
Tag antenna gain, G_T	0 dBi (omni-directional)
Channel bandwidth B	200 KHz [2]
Noise figure, F	10 dB [22]
$P_{sens,T}$	-15 dBm [22]
Noise power spectral density	-174 dBm/Hz [15]
Wall Attenuation	12 dB
d_m	1 m
Reading time per tag, t_r	3 ms
MAC Parameters	
τ_{arr}	100 ms
Carrier sense threshold (for both LBT and CSMA)	-96 dBm
CSMA/CA Parameters	
timeslot	5 ms
DISF	15 ms
CW_{min}	75 ms
CW_{max}	5115 ms
Scheduler Parameters	
T_{beacon}	0.5 s
α	0.5
β	0.3

The bar plots in Fig. 7, Fig. 8 and Fig. 9 show the simulation results concerning the access delay. These plots refer to the average access delay (Fig. 7), the standard deviation of the average access delay (Fig. 8) and the maximum access delay (Fig. 9), respectively.

As it is possible to see from the plot in Fig. 7, the readers do not experience any delay when using Aloha, as this access technique does not require the readers to wait for the channel to be idle before the transmission. LBT performs better than CSMA and HF-RACP, but this small performance loss is anyway repaid in terms of much higher collision efficiency of the latter. Indeed, though the average delay is low, the number of collisions experienced by the readers adopting LBT is quite high. If we only focus on the two algorithms with the best collision avoidance performance, that is, CSMA and HF-RACP, the latter exhibits lower access delay to the channel. Depending on the scenario, the reduction of the average access delay of HF-RACP compared to CSMA ranges from 36% up to 46%. The reason for the much higher delay in case of Scenario 1 compared to Scenarios 2 and 3 is the higher number of readers (20 in case of Scenario 1 and 9 in case of Scenarios 2 and 3). The higher the number of readers, the higher is the number of contenders to the channel. Thus, on average, each reader has to wait for a longer time for the channel to become idle. HF-RACP improves also the fairness among readers. The fairness here is meant as an even possibility of all the readers to access the channel. If some reader experiences higher access delay than others, the latter readers have clearly some advantage with respect to the former. This means that the algorithm does not provide enough fairness among the readers.

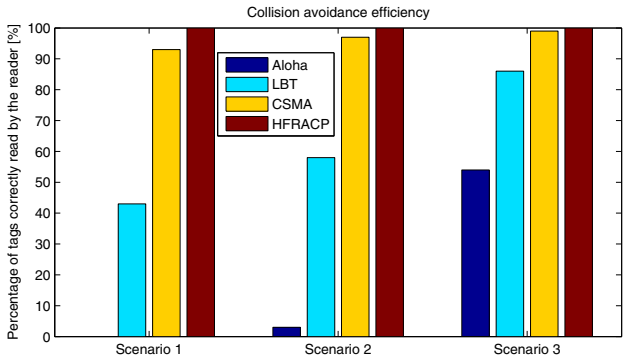

Fig. 6: Collision avoidance efficiency results.

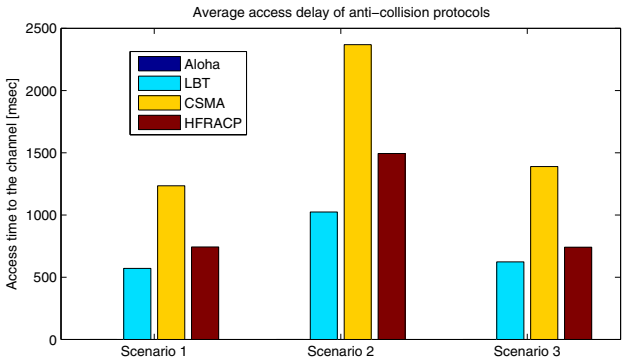

Fig. 7: Average access delay simulation results.

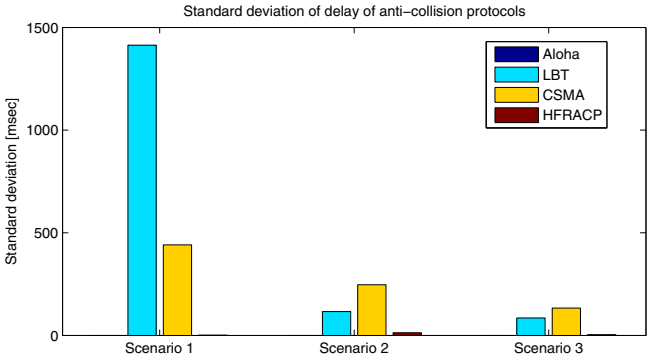

Fig. 8: Standard deviation of access delays.

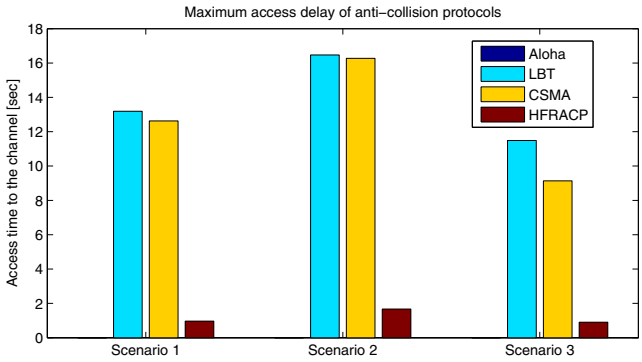

Fig. 9: Maximum access delay simulation results.

As we can see from Fig. 8, HF-RACP shows a standard deviation of the delay which is close to 0, meaning that all the readers exhibit almost the same mean access delay and there is a high fairness among the interrogators. On the contrary, LBT and CSMA show much higher standard deviation of the delay, that is, there is a large difference between the mean access delays of each reader. Compared to LBT and CSMA, HF-RACP reduces the standard deviation of the delay about 8-15 times in Scenario 1, about 20-30 times in Scenario 2 and up to 30-100 times in Scenario 3. The comparison with the standard deviation of Aloha is meaningless, since Aloha has no access delay.

The HF-RACP is effective also for reducing the maximum access delay. As it can be seen from the plot in Fig. 9, the maximum access delay experienced by the readers using HF-RACP is much lower than the delay experienced with LBT and CSMA. As it was expected, by means of allocating the readers with higher access delay, the scheduling algorithm prevents the access delay of the readers to reach unwanted peaks, as it occurs in case of LBT and CSMA. In fact, the maximum access delay is reduced about 10-13 times with respect to LBT and CSMA in the considered scenarios.

Overall, the centralized scheduling of the readers proposed in this paper showed to be effective against the reader collision problem, as the collision avoidance efficiency is close to 100% in all the simulated scenarios. Furthermore, the scheduling improves the fairness among the readers and reduces the peak access delay compared to LBT and CSMA.

VI. Conclusions and Future Work

In this paper, a solution for the reader collision problem in passive RFID systems has been provided. The proposed anti-collision protocol has been simulated and compared with other solutions as far as it concerns the collision avoidance efficiency and the access delay for three different indoor scenarios. The proposed solution has been proved to be effective against the reader collisions in all the considered scenarios, as the collision avoidance is close to 100%. Furthermore, the scheduling algorithm improves the fairness among the readers when accessing the channel and it limits the maximum access delay. The reduction of the standard deviation of delay (as a measure of unfairness) with respect to LBT and CSMA algorithms ranges from 10 up to 100 times depending on the scenario, while the reduction in maximum access delay is in the order of 10.

The next steps of this work will include the study of the impact of the overhead introduced by the collision discovery algorithm on the access delay performance of HF-RACP.

VII. Acknowledgements

This work has been carried out within the framework of the FP7 ASPIRE (Advanced Sensors and lightweight Programmable middleware for Innovative Rfid Enterprise applications) project (http://www.fp7-aspire.eu/rfid/).

References

[1] S. Ahson and M. Ilyas, *RFID Handbook: Application, Technology, Security and Privacy*. CRC Press, 2008.

[2] EPCGlobal, "EPC Radio-Frequency Identity Protocols Generation 2 Identity Tag (Class 1): Protocol for Communications at 860 MHz-960 MHz," 2008, http://www.epcglobalinc.org/standards/uhfc1g2.

[3] S. M. Birari and S., "Mitigating the Reader Collision Problem in RFID Networks with Mobile Readers," *IEEE International Conference on Networks*, vol. 2, 2005.

[4] D. Engels and S. Sarma, "The Reader Colision Problem," *IEEE International Conference on Systems, Man and Cyberbetics*, pp. 1–6, October 2002.

[5] H. B. Chung, H. Mo, N. Kin, and C. Pyo, "An Advanced RFID System to Avoid Collision of RFID Reader, Using Channel Holder and Dual Sensitivity," *Microwave and Optical Technologies Letters*, vol. 49, pp. 2643–2647, November 2007.

[6] K. H. Junius, "Solving the Reader Collision Problem with a Hierarchical Q-learning Algorithm," Master's thesis, Massachusetts Institute of Technology, February 2003.

[7] D. Klair, K.-K. Chin, and R. Raad, "A Survey and Tutorial of RFID Anti-Collision Protocols," *IEEE Communications Surveys & Tutorial*, vol. 12, pp. 400–421, 2010.

[8] "ETSI EN 302 208-1 v1.1.1 (2004-09)," www.etsi-org.

[9] J. Waldrop, D. W. Engels, and S. E. Sarma, "Colorwave: An Anticollision Algorithm," *ICC'03 IEEE International Conference on Communications*, pp. 1206–1210, 2003.

[10] C.-H. Hsu, S.-C. Chen, C.-H. Yu, and J.-H. Park, "Alleviating Reader Collision Problem in Mobile RFID Networks," *Personal and Ubiquitous Computing*, vol. 7, pp. 489–497, April 2009.

[11] J.-B. Eom, S.-B. Yim, and T.-J. Lee, "An Efficient Reader Anticollision Algorithm in Dense RFID Networks With Mobile RFID Readers," *IEEE Transactions on Industrial Electronics*, vol. 56, pp. 2326–2336, July 2009.

[12] C.-H. Quan, J.-C. Choi, G.-Y. Choi, and C.-W. Lee, "The Slotted -LBT: a Dense Reader Medium Access Scheme in Dense Reader Environment," *IEEE, International Conference on RFID*, 2008.

[13] C. Galiotto, N. Marchetti, N. R. Prasad, and R. Prasad, "Low Access Delay Anti-collision Algorithm for Readers in RFID Systems," *The 13th International Symposium on Wireless Personal Multimedia Communications (WPMC)*, October 2010.

[14] M. Monsen, "Radio Frequency Identification (RFID): Potential Impacts on Information Technology Equipment (ITE)," December 2009, http://www.ist-winner.org/WINNER2-Deliverables/D1.1.2.zip.

[15] N. Benvenuto and G. Cherubini, *Algorithms for Communications Systems and Their Applications*. John Wiley & Sons, August 2002.

[16] Y. Han and H. Min, "System Modeling and Simulation of RFID," 2005, http://www.autoidlabs.org/uploads/media/AUTOIDLABS-WP-HARDWARE-010.pdf.

[17] Y. Liu, K. Contractor, and Y-Kang, "Path Loss for Short Range Telemetry," *4th International Workshop on Wearable and Implantable Body Sensor Networks*, vol. 13, pp. 70–74, 2007.

[18] K. S. Leong, M. L. Ng, and P. H. Cole, "Positioning Analysis of Multiple Antennas in a Dense RFID Reader Environment," *International Symposium on Applications and the Internet Workshops, SAINT*, 2006.

[19] C. Floerkemeier and S. Sarma, "RFIDSim - A Physical and Logical Layer Simulator Engine for Passive RFID," *IEEE Transaction on Automation Science and Engineeing*, vol. 6, January 2009.

[20] T. Rappaport and C. McGillem, "UHF Fading in Factories," *1989*, vol. 7, no. 1, January 1989.

[21] U. Karthaus and M. Fischer, "Fully Integrated Passive UHF RFID Transponder IC with 16.7-μW Minimum RF Input Power," vol. 38, October 2003.

[22] D.-Y. Kim, H.-G. Yoon, , and B.-J. Jang, "Effects of Reader-to-Reader Interference on the UHF RFID Interrogation Range," *IEEE Transaction on Industrial Electronics*, vol. 56, no. 7, pp. 2337–2346, July 2009.

[23] B. Sklar, *Digital Communication. Fundamentals and Applications*. Prentice Hall, 2001.

[24] A. I. Barbero, G. D. Horler, E. Rosnes, and O. Ytrehus, "Modulation Codes for Reader-Tag Communication on Inductively Coupled Channels," *Proc. Int. Symp. Inf. Theory and its Appl. (ISITA), Auckland, New Zealand*, pp. 578–583, December 2008.

[25] H. Labiod, H. Afifi, and C. D. Santis, *Wi-Fi, Bluetooth, Zig-Bee and Wi-Max*. Springer, 2007.